International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Steganography in High Intensity Pixel of a Thermal Image using Barcode Encoder Technique

S.Rathika, R.Gayathri

Abstract: ***In this research, the high intensity pixels are the region of interest is selected based on the difference in the intensity level of the colors in an image. The image holding the information is hidden in a cover image which is pattern locked in which a random number is allocated for each of the pixel. The pattern is drawn and the nodes that connect each pixel were selected and marked as the area of interest, which has high intensity as said. These numbers extracted and converted to barcode that are saved as normal image. In this proposed research the information that is hidden in the normal image is fused with the thermal image, which comprises of high intensity colors. The image fusion technique which is proposed in this research is much interesting that ensures more security as it do not reveals any clue about the existence of the information to interpreters. This research, analyzes the Barcode Encoder technique in steganography only on colors with high intensity, and identifies those areas where this technique can be applied, so that the human race could be benefited abundantly.***

Key points: Cryptography, Steganography, Barcode Encoder.

I. INTRODUCTION

Information hiding, received more attention in the modern digital era, because security of information has become an important concern in this internet world. Sharing of sensitive information through a common communication channel has become inevitable; Steganography [10] in image processing is a simple and secure method for transferring confidential information. Various analyses has been experimented and verified to ensure the absence of any hint on the stored data. In this proposed method, we have analyzed the color based Steganography [12] on a specific area in an image holding high intensity colors. This research uses Thermal image as an Input image for numerous reasons. Thermal imagers can be used to image objects both large and small such as tanks deployed on the battlefield (landscape scale) to components that comprise a printed circuit board. They are infrared radiation detectors that may be used to perform noncontact thermal mapping of any device, system, object, or animal that emits infrared radiation (heat).The main advantage of thermal images over visible aerial photography is heat sensing. Thermal Image [5]

Manuscript published on 30 September 2019
* Correspondence Author
Mrs. S.Rathika*, Research Scholar, Dept. of ECE, Annamalai University, Tamilnadu
Dr.R.Gayathri, Assistant Professor, Dept. of ECE, Annamalai University, Tamilnadu

steganography can be implemented in Video data hiding with high data rate, where the thermal image can be converted into [9] color image and can also be used on temperature monitoring of power transformers. The chosen block is converted to a grey valued image after hiding the data. To ensure the security furthermore a key is used to lock the cover image. Basic Block diagram of the proposed research is in the following figure 1.

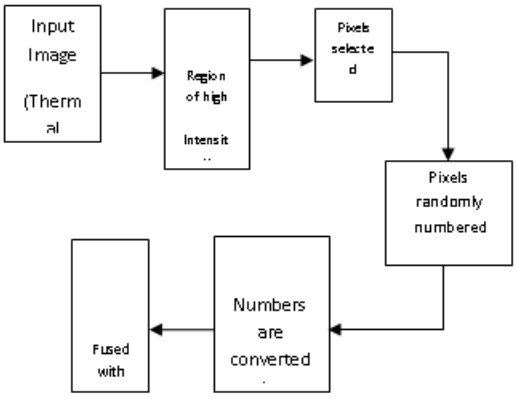


Fig 1. Basic Block Diagram

In the block diagram the first block is explaining the information that has to be hided is kept in the thermal image as an input image. In the second block from the RGB format Blue color is selected as High intensity region. Then pixels with high intensity [14] are selected and numbered randomly. Then the numbers are bar-coded and at last this thermal image is fused with normal image to ensure high security while transforming the data through steganography.

2. Selecting High Intensity Region

Image Steganography [11] is the method of embedding text in images in a way that its presence cannot be detected by Human Visual System (HVS) and is known only to the sender and the receiver. An advanced approach for image steganography using Hue-Saturation-Intensity (HSI) color space based on Least Significant Bit (LSB) [1] has been proposed in the above mentioned paper. Here the proposed method transforms the image from RGB color [2] space to Hue-Saturation-Intensity (HSI) color space and then embeds the secret data inside the Intensity Plane (I-Plane) and transforms it back to RGB color model once embedding. The color image when read by the computer, are converted in a machine language, say 1s and 0s. The sequence of those bits in a stream line of standard pattern is understood as an image by the system. Each color [13] is represented as a binary number and each decimal number over here will be holding a color that the system understands in a binary format. The weight age of all colors in an image can be identified by converting the color value into a decimal number. In this proposed system the highest intensity color alone is selected say R, G & B. In this research we selected blue color from the image instead of cryptography as it concentrates on retaining message contents secret, the steganography [8] concentrates on the secrecy of the existence of a message.

The following figures 2 and 3 showing the normal color image and the high intensity thermal image of the proposed paper.

Fig 2

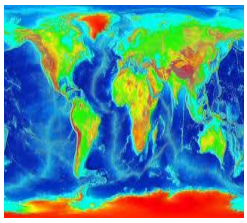


Fig 3

A high security and robust approach of information security is proposed which represents two component based LSB (Least Significant Bit) methods for embedding secret data in the LSB's [4] of blue components and partial green components of random pixel locations in the edges of images; whereas in this research, the color [7] concentrated is numbered and manipulated further to ensure high security.

3. Numbering and Pixel selection

A group of regions which hold the specific color is selected say an 8X8 matrix. Since the same range of colored value are presented in the neighborhood pixels, any changes or manipulations done in the Least Significant Bits is untraceable and so it will provide high security for the hidden data, when it is performed in single digit count on 8X 8 pixels, in an image of very high resolution. The hexadecimal values of all the colors stands between 00000000 - 1111 1111, for an 8 X 8 matrix, where each pixel is assumed to hold an 8 bit value, whose decimal count ranges from 0 to 255. With the region selected in an image the very minute differences is noted where the color ranges from 10-60 which was unnoticeable even when it is manipulated at its least four bits. Based on the color value they are numbered as given below. The sequence of the pattern drawn is reversed as 14/31/18/13/26/52. This sequence is bar coded and those selected pixels color value is numbered and the secret data sequence is taken where the sequence shows a pattern method drawing at the user's interest.

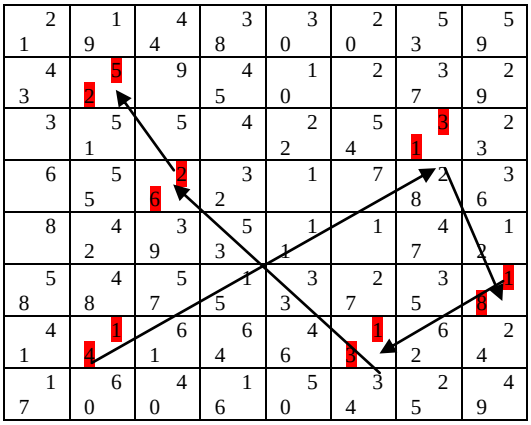


Fig 4. Pattern drawn on 8x8 Matrix

Any pattern can be drawn as the same from four moves to 64 steps of the sixty four factorial methods. The LSB of these locations are modified to indicate the receiver that the manipulation is done on these pixels, and the sequence is also hidden in the cover image after converting it to a barcode image.

4. Barcode from Numbers

The barcodes are the one where we can hide the data and those data will be reached safely to the authorized person without disclosed to others in the middle. The barcodes are mainly made up of bars and squares in the black and white color format. In 3D barcodes the third dimension will be added as the color. The main reason for introduction of these 3D barcodes is high temperature resistant. The barcode converter is used to convert the input sequence including the space(_) or back slash (\) or a slash (/), or semi colon (;) anything that is used to separate the decimal sequence count. The sequence plays an important role of delivering the secret pattern drawn. Hence, this is also demanding authentication, hence in this method, the sequence can be reversed if needed as front end back.

14/31/18/13/26/52

It is an easy cryptographic technique where this can have six factorial combinations again the converted sequences are saved in any one of the formats discussed above as an image. By mixing the contribution of each component, a large palette of colors can be represented in the stego image.

Fig 5. Barcode Image of the sequence.

In this method high capacity barcode [6] can be generated instead of 2-D image, where lot of information can be hidden at the best.

5. Fusion of Stego Image with a password

Image fusion generates a composite image by integrating the complementary information from multiple source images in the same scene. The input source image in an image fusion system is non-inheritable either from numerous varieties of image sensors or from one sensor with different optical parameter settings. So the fused image as output is more suitable for human visual perception and machine processing than any single source image. Image fusion techniques have been widely used in computer vision, surveillance, medical imaging, and remote sensing, and so on.

This barcode image is fused with the normal image which is the stego image that holds the image of the manipulated selected color valued pixels, which gives the pattern drawn or password entered, collectively to the receiver. The fusion of barcode image and the blue colored image with the normal image gives the stego image. The Most significant bits of the secret data hidden image are stored in the LSB of cover image, which gives no clue about the existence of the information in the cover image. Thus, the resultant image is further locked using a 4 bit password to enhance the security level, and pays the receiver with authenticity to decode the stego image and get back the original information.

6. Fusion – Visual Vs Thermal Image

The fusion of visual and thermal image is done to hide the information data in the thermal image and to protect the thermal image inside the visual image. The designated receiver should be using the same technique to decode the thermal image from the visual image. Later the thermal image is processed to decode the secret information hidden. Least Significant bit algorithm used to fuse both the images based the weight of the images.

```
if use_greyscale
   test_name = ['Fusion_', carrier_image_filename, '_thermal'];

Else

   test_name = ['Fusion_', visual_image_filename];

End
```

Fig 6. Visual Image

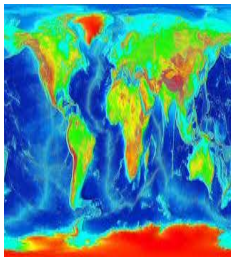


Fig 7. Thermal fused- Barcode Image

Fig 8. Fused (Visual and Thermal) Image

The above fused image gives no clue of the existence of the thermal image inside, and the information hidden either.

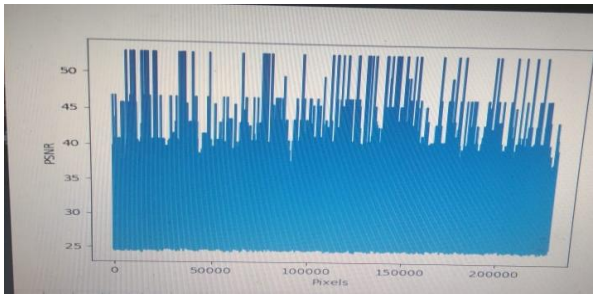
7. Test Results and Analysis

Quality metrics [3] analysis (PSNR, MSE) is an important work in digital image processing as it provides a better way for image quality assessment and its improvement.

```
import numpy
import math
import cv2
original = cv2.imread(r"C:\Users\nibsz\Desktop\Projects\stego\hidden_iiiii.png")
contrast = cv2.imread(r"C:\Users\nibsz\Desktop\Projects\stego\final_hidden_iiii.png",1)
def psnr(img1, img2):
    mse = numpy.mean( (img1 - img2) ** 2 )
    print('MSE =',mse)
    if mse == 0:
        return 100
    PIXEL_MAX = 255.0
    return 20 * math.log10(PIXEL_MAX / math.sqrt(mse))

d=psnr(original,contrast)
print('PSNR =',d)
```

PSNR and MSE of the output image is as follows,



MSE = 104.39210552947337 PSNR = 27.944127037210357

8. Conclusion

By altering the intensity of any image, the intention towards the attraction is reduced. The information image is converted to grey level usually to ensure the authentication of secret communication or for any manipulations in image processing. This process of hiding algorithm helps in locking the secret data with multiple stego and crypto process. The analyzed technique that hides sequence of data provides successful implementation and verified with a better image quality. Further, this research shall be extended for video signals and also with audio signals, which would be more useful for the real time applications where secret communications are more necessary.

REFERENCES

1. Jain, Ahirwal. A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys. International Journal of Computer Science and Security (IJCSS). 2010 March; 4(3):111-119.
2. R.Amirtharajan, Sandeep Kumar Behera, Motamarri Abhilash Swarup, Mohamed Ashfaq K & John Bosco Balaguru Rayappan, 2010, "Color Guided Color Image Steganography", Universal Journal of Computer Science and Engineering Technology, vol 1, no.1, pp. 16-23, Oct. 2010.
3. Chauhan N, Waoo AA, Patheja PS. Attack detection in watermarked images with PSNR and RGB intensity. International Journal of Advanced Computer Research. 2013; 3(1):41-5.
4. Vrishali Chakkarwar, Bhagyashri Patil, "Review of an Improved Audio Steganographic Technique over LSB through Random Based Approach" IOSR Journal(ISORJCE),VOL:9 Issue 1, Jan–Feb 2013.
5. Kirk J. Havens, Edward J. Sharp, in Thermal Imaging Techniques to Survey and Monitor Animals in the Wild, 25th September 2015.
6. J. Duda, P. Korus, N. J. Gadgil, K. Tahboub and E. J. Delp, "Image-Like 2D Barcodes Using Generalizations of the Kuznetsov–Tsybakov Problem," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 4, pp. 691-703, April 2016.
7. J. Wen, J. Zhang, J. Zhou, Y. Li and Y. Xue, "An Adaptive JPEG Steganographic Scheme Based on Run-Length Statistical Complexity," in Chinese Journal of Electronics, vol. 27, no. 1, pp. 52-59, 1 2018
8. M. Rajput, M. Deshmukh, N. Nain and M. Ahmed, "Securing Data Through Steganography and Secret Sharing Schemes: Trapping and Misleading Potential Attackers," in IEEE Consumer Electronics Magazine, vol. 7, no. 5, pp. 40-45, Sept. 2018.
9. U. S. Kumar and N. M. Sudharsan, "Enhancement techniques for abnormality detection using thermal image," in The Journal of Engineering, vol. 2018, no. 5, pp. 279-283, 5 2018
10. X. Zhang, F. Peng and M. Long, "Robust Coverless Image Steganography Based on DCT and LDA Topic Classification," in IEEE Transactions on Multimedia, vol. 20, no. 12, pp. 3223-3238, Dec. 2018.
11. X. Qin, B. Li, S. Tan and J. Zeng, "A Novel Steganography for Spatial Color Images Based on Pixel Vector Cost," in IEEE Access, vol. 7, pp. 8834-8846, 2019.
12. J. Lu, G. Zhou, C. Yang, Z. Li and M. Lan, "Steganalysis of Content-Adaptive Steganography Based on Massive Datasets Pre-Classification and Feature Selection," in IEEE Access, vol. 7, pp. 21702-21711, 2019.
13. K. Chen, H. Zhou, W. Zhou, W. Zhang and N. Yu, "Defining Cost Functions for Adaptive JPEG Steganography at the Microscale," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 4, pp. 1052-1066, 2019.
14. Z. Zhao, Q. Guan, H. Zhang and X. Zhao, "Improving the Robustness of Adaptive Steganographic Algorithms Based on Transport Channel Matching," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 7, pp. 1843-1856, 2019.

AUTHORS PROFILE

Ms. S. Rathika, is pursuing her Research in Thermal Image processing from ECE Department at Annamalai University, Chidambaram, She is working as an Associate Professor in Prince Shri Venkateshwara Padmavathy Engineering College, Chennai. Her Research interests includes Cryptography and steganography in Thermal Image Processing,

Dr. R. Gayathri, Asst Prof of ECE, Annamalai University has authored several papers in indexed International Journals and Conferences. Her area of interest includes Microwaves, Antennas, Image Processing and Networks. She is Reviewer of reputed International Journals. She is member of many Engineers society.